N

NetStalker™

Installation and User's Guide

Version 1.0.2

Haystack Labs, Inc.

10713 RR 620 North, #521
Austin, TX 78726
512-918-3555
512-918-1265 FAX

5/96 NETSTALK

THE *NETSTALKER* ™ INSTALLATION AND USER'S GUIDE DOCUMENT REVISION 1.0.2

NetStalker was created by: Steve Smaha, Steve Snapp, Jessica Winslow, Richard Letsinger, Crosby Marks, Charisse Castagnoli, Brita Womack, and Kristin Johnson.

Contents

List of Figures

List of Tables

CHAPTER 1

Introducing *NetStalker*™

This chapter introduces *NetStalker* network monitoring software from Haystack Labs, describes what *NetStalker* does, and its relationship to Network Systems Corp. (NSC) routers.

Introducing *NetStalker*

What is *NetStalker* and what does it do for you? *NetStalker* provides real-time monitoring and analysis of network events. This chapter defines these commonly used terms and describes several scenarios that illustrate how *NetStalker* works in your world.

Product Overview

NetStalker monitors all events reported from client SSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real time using information stored in an internal database, the misuse signature database. Depending on how you configure *NetStalker*, it can also generate detailed reports from the recorded data. These reports provide information suitable for either or for a technical review.

Consider this example

Your company "Specialized Software Corporation" (SSC) has obtained an Internet connection to allow users to access files stored in your library of software examples and patches (via ftp), and engineers working at remote sites to access information on their systems.

SSC is sensitive to the fact that a hacker may get in to the system, and is using a Network Systems Corp. router configured with *NetStalker* to protect the system from attack -- while allowing unrestricted access for legitimate users. Here are some scenarios that describe how *NetStalker* protects the internal network and watches for attacks, but permits legitimate users to go about their business.

Scenario 1:

Legitimate ftp access: A registered user of SSC's software tries to ftp a software patch from their public access system (ftp.sscorp.com). The connection is logged (so that SSC has a record of accesses to the patch server that were distributed). The file transfer is permitted and successful.

Result: A legitimate outside user can successfully access public files without interference. To enable ftp monitoring, run the *NetStalker* configuration FTP_watch.

Scenario 2:

Legitimate system access: Sue is trying to get her program to run on the floor of a trade show. She needs to access a special configuration file on her system back at SSC. Using telnet, she connects to her system (rushmore.ssc.com) from the floor system which uses a known IP source address, and obtains her file successfully.

Result: An employee can successfully access her system remotely without interference. To monitor all telnet sessions, run the *NetStalker* configuration Telnet_watch.

Scenario 3:

An attempt to break in via ftp from a bad host: A hacker has been reading about SSC and realizes that the proprietary information stored in the SSC systems is extremely valuable, especially to competitors. The hacker has been wandering the floor at a trade show and notes the name of the system that Sue logged on to (rushmore.ssc.com). As a first attempt, the hacker tries to make an ftp connection to rushmore.ssc.com. *NetStalker* records the illegal ftp access attempt and reports the violation.

Result: The router blocks the illegal access attempt. *NetStalker* sends an alarm to the SSC system/network administrator. To monitor bad ftp attempts, run the *NetStalker* configuration Blocked_FTP_Session.

Scenario 4:

An attempted break-in via IP spoofing: Since the first attempt was unsuccessful, the hacker tries another approach. Setting his system's IP address to that of rushmore.ssc.com (the system to which Sue is logged on), he tries to log into the network again, attempting to trick the system into believing that he is logging in from a "legitimate" node within the network. *NetStalker* identifies this as a request that appears to be coming from inside the company, but is physically coming from outside -- an attempted "IP spoof."

Result: The router blocks the illegal access attempt. *NetStalker* sends an alarm to the SSC system/network administrator. To monitor IP spoofing attempts, run the *NetStalker* configuration IP_Spoof.

Scenario 5:

Attempted break-in via rsh/rlogin: In his third attempt, the hacker sets up an account called "sue" on his own machine, and attempts to use rlogin to break in to rushmore.ssc.com. If Sue has left an open .rhosts file on her system, this may let the hacker in. *NetStalker* records rsh and rlogin attempts and reports the violations.

Result: The router blocks the illegal access attempt. *NetStalker* sends an alarm to the SSC system/network administrator. To monitor r command connections, run the *NetStalker* configuration r_command_watch.

Scenario 6:

Attempted break-in via illegal port: As a final attempt, the hacker tries to break in by creating an illegal X terminal session. The hacker goes by SSC's booth and notices that Sue is remotely logged in to her system, and that she has walked away from her terminal. The hacker uses the opportunity to generate a remote X terminal session from Sue's login shell on rushmore. The hacker tries to start an X-terminal session back to the trade show floor. *NetStalker* records the access via the illegal port and reports the violation.

Result: The router blocks the illegal access attempt. *NetStalker* sends an alarm to SSC system/network administrator. To monitor X-session requests, run the *NetStalker* configuration X-session_watch.

At this point, the system administrator at SSC has received multiple notifications from the attempted illegal accesses. He can now take corrective action to further secure his systems.

NSC Clients and How They Interface with *NetStalker*

Initial PCF filter configuration

NetStalker has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and *NetStalker*. The filters are created and downloaded to the router when you run the shell, INSTALL.filters. See Chapter 2 for information on installing *NetStalker*.

Receiving data from router

Console redirect messages are sent by the NSC client to socket 1780. PCF copyto messages are received by *NetStalker* on socket 1781.

Controlling router

A Unix shell-accessible program turns on or turns off a router-based shunning response. A shunning response is an instruction to the router to reject all packets from a specified individual IP address. This shunning response is controlled from the *NetStalker* user interface. See Chapter 4 for information on creating a shunning response.

Securing the connection

Since the *NetStalker* server platform can be located anywhere on the network, there is the potential of an attacker manipulating the connection between the router and the *NetStalker* server platform.

The most efficient means of protecting this connection between the NSC router client and the *NetStalker* is to use separate BorderGuard routers between the *NetStalker* platform and the network, and then to configure an encrypted tunnel between the client router and the "guard" router that protects the *NetStalker* platform. Since all IP traffic between the *NetStalker* platform and client is encrypted on the network, the encryption provides confidentiality, integrity, and mutual authentication of the communicating parties.

Alternatively, the *NetStalker* platform can be located on an individual network segment that is directly connected to a dedicated port on the router it is monitoring.

Supported *NetStalker* Clients

A *NetStalker* client is the network device being monitored by *NetStalker.* Refer to the release notes that are shipped with your copy of *NetStalker* for specific information on:

- The number of client routers supported by one copy of *NetStalker*
- Specific router models supported
- Hardware and software requirements
- Other changes to *NetStalker* that are not covered in this manual

CHAPTER 2

Getting Started

This chapter describes

- Prerequisites
- Installing the Software
- Starting *NetStalker*
- Iconifying *NetStalker*
- Stopping *NetStalker*
- *NetStalker* menus

Prerequisites

NetStalker must be installed on a workstation designated as the *NetStalker* server. For specific hardware and software requirements, refer to the release notes distributed with your software.

Installing *NetStalker*

NetStalker Package

The complete *NetStalker* set consists of a software media distribution, this Installation and User's Guide, and Release Notes. In addition, *NetStalker* includes extensive on-line help that is accessible from the graphical user interface, plus standard Unix man pages for command line use.

NetStalker installation media will not execute until an installation program is run with a valid cryptokey. In the event the *NetStalker* workstation hostid changes (either through a modification of the workstation's motherboard or when a customer wants to move *NetStalker* to another workstation), a new cryptokey must be generated by NSC and the customer must reinstall *NetStalker*.

NetStalker's GUI

NetStalker is built as a Motif application using the X Windows interface. It runs under either Motif or OpenLook. All X resources are given default values which you can modify.

NetStalker operates as an X application with a mouse, graphical display device, and keyboard, and does not support "dumb terminal" (tty) operation. As an interactive application, its individual windows can be iconized to reduce screen utilization.

Privileged Access

NetStalker must be installed by the root login in order to place configuration files in protected directories.

Setting up the Environment

To install *NetStalker*, you must

- Have an account for the userid that will normally run *NetStalker* and a crontab file for the account.
- Have access to the root password. If you do not have access to the root password, contact technical support.
- Backup your router

It takes about 15 minutes to install *NetStalker*.

To set up the environment, follow these steps:

1. Type `su root` and press **Enter**.
2. Type the root password and press **Enter**.

3. On a local disk create the following directory, **mkdir $NETSTALKERHOME** and press **Enter**. This directory is the target directory where *NetStalker* will be installed.
4. Type **chmod 750 $NETSTALKERHOME** and press **Enter**.
5. Type **chown userid $NETSTALKERHOME** and press **Enter** (where userid is the userid that will normally run *NetStalker*.

Loading from tape

NetStalker is shipped on one tape that includes versions for all supported operating systems. You must fast forward the tape to the appropriate operating system using the appropriate command, as shown in Table 2-1.

TABLE 2-1 Fast Forward Commands

OS	Fast Forward Command
Solaris	`mt -f /dev/rmt/0n fsf 1`
SunOS	`mt -f /dev/nrst0 fsf 2`
IBM/AIX	`mt -f /dev/rmt0.1 fsf 3`
HP-UX	`mt -f /dev/rmt/0mn fsf 4`

To extract *NetStalker* from a tape, follow these steps, using the appropriate tape device for your operating system. The tar command extracts the *NetStalker* directory from the tape and places it in the current directory.

1. Type **cd $NETSTALKERHOME** and press **Enter**.
2. Insert the *NetStalker* tape into the drive.

   On most machines the tape is **/dev/rst0**. If your tape drive has a different name, adjust these instructions accordingly.
3. Type **tar xvf /dev/rst0** and press **Enter**. This tar command unloads *NetStalker* from the tape and places it in the current directory.
   Here is an example of what you see on your screen as the files are extracted:

```
#tar xvf /dev/rst0
x ./bin/netstlkr.exe, 2464824 bytes, 4815
tape blocks
x ./bin/dbbuild.exe, 1915960 bytes, 3743
tape blocks
.
.
.
x ./INSTALL
```

Look through the transcript that the tar command displayed to make sure that each file was transferred correctly. If the tar command reports an error, the error begins with `tar`: as follows:

```
tar: can't create...
```

If you get an error, verify the directory permissions and try again. If the error persists contact technical support.

4. Type **`chown -R userid *`** and press **Enter**. This command sets the ownership of all *NetStalker* files.

Run the installation script

To run the installation script, do the following:

1. Have available the IP address and the network mask of the internal network that *NetStalker* will monitor.
2. Type **`./INSTALL`**
3. When presented with this or similar message:
   ```
   NetStalker's user interface uses an
   application defaults file for displaying
   fonts and colors. This file can be installed
   into the directory /usr/openwin/lib/app-
   defaults. Do you want to install the
   defaults?
   ```
   Answer **`yes(y)`** to this question; otherwise some fonts and colors will be undesirable or unusual. The directory name varies by operating system.
   ```
   Do you want soft colors?
   ```
   Answer **`yes(y)`** to this question if you prefer subdued colors, answer **`no(n)`** if you prefer primary colors.
4. When presented with the message:
   ```
   What is the userid of the user that will be
   running NetStalker?
   ```
   Enter the appropriate userid or accept the default userid **`stalker`**.
5. *NetStalker* needs to know the difference between the inside monitored network and outside. When prompted, type your internal network IP address here. The network address must be in dotted quad notation with "*" for the host portion of the address. e.g. 192.28.*.* or 198.*.*.*
6. When prompted, enter the customer key.
7. Record the checksum in Appendix A.
8. Now exit the root account.

Gather Network Information

Before installing the *NetStalker* filters on the router, collect the following information:

1. The IP address of the workstation where *NetStalker* runs
2. The name of the router *NetStalker* is monitoring
3. The Router password
4. The Router IP address

If you do not have this information, contact technical support before attempting to install the *NetStalker* filters.

Test Router

Before installing the *NetStalker* filters on the router, test your connectivity to the router to ensure the server and the router can communicate.

1. Type `ping routername`
   This will tell you if a communication path exists between the router and the *NetStalker* server.
2. Type `telnet routername`
   This will tell you if you have the proper password for the router.
3. Verify the tftp connection using the telnet session created in step 2. See the man pages for your operating system to enable tftp. Type `ip` and press **Enter**.
4. Now you can try to tftp a file from the *NetStalker* server to the router.
   Type `tftp` and press **Enter**.
5. Type `connect NetStalker server` (**Note.** This must be the IP address of the *NetStalker* server.)
6. Type `get $NETSTALKERHOME/filters/get_adr.s`
   If this command is successful you can tftp from the router.

Run the Filter Installation Script

To run the script for installing filters on the router, do the following:

1. Type `cd $NETSTALKERHOME/filters` and press **Enter**.
2. Type `./INSTALL.filters` and press **Enter**. The INSTALL.filters script will ask you several questions to configure your system properly.
3. When presented with the message:
   `What is the IP address of the NetStalker server?`
   Enter the IP address of the *NetStalker* server and press **Enter** or press **Enter** to accept the default IP address.

4. When presented with the message:
   `What is the IP address of your secure network?`
   Enter the IP address and press **Enter** or press **Enter** or accept the default address entered in Step 5 of the Installation Script.
5. When presented with the message:
   `What is the name of the router?`
   Enter the router name and press **Enter** to put the filters into place. The Security Router and the 6600's display the name on the front panel LCD screen. For the name of the BorderGuard router, you must telnet to it and read it from the system prompt. If no name is set, insert the following into the router's start-up file:
   `set name "routername"` and press **Enter.**
6. When presented with the message:
   `What is the IP address of the router?`
   Enter the IP address and press **Enter** or press **Enter** to accept the default.
7. Enter the number that corresponds to the router type.
   ```
   What is the IP address of the router?
   1) BorderGuard
   2) Security Router
   3) DX/DXE/6600
   4) ERS
   ```
8. Type **y** or **n** about the version of PCF running on the router.
9. In order to install the filters you must enter the router password. Enter it here. If no password is set, press return. Either way, you are prompted to enter the password a second time.
10. FOR HP-UX INSTALLATION ONLY:
    You are asked to enter the path of the tftp directory for the *NetStalker* server.
11. At this point, *NetStalker* creates custom filters and copies them to the router. If any problems occur, the file can be copied over manually using Router commands. Each .fil file in the filters directory should be copied to the router.

Warning — Do not modify filters whose name begins with "stalker". Do not modify the router's logging mechanism although you may set the console log severity level for interactive telnet sessions.

Applying PCF Filters at the Router Follow these steps to permanently apply PCF filters on all routers except the ERS. See the Release Notes for instructions on applying filters to the

ERS router.

1. Modify the startup file to run the *NetStalker* filters as shown in the following example. You should copy your existing startup file before you begin editing.

   Because of the many possible variations in filters for an NSC router, this description assumes a new "pristine" NSC router.

   Assume the router is named "foo" and has two interfaces.

   Interface 1 (en01) has IP address 198.51.45.253 and is attached to the "inside" secure network.

   Interface 2 (en02) has IP address 192.9.200.254 and is attached to the "outside" insecure network.

   This startup file installs several *NetStalker*-specific files. The first three lines of the sample file must be in place as the first three lines of the actual startup file. The *NetStalker* specific information is identified by italics.

   Sample file listing:

```
set name "foo"
@stlkcomp.cmd
ip apply netstalker on first

# Connected to internal network
ip start if en01 198.51.45.231 netmask
0xffffff00

# Connected to outside world
ip start if en02 192.9.200.254 netmask
0xffffff00 \
incoming=stalker_ip_spoof_fail

#Startup packet forwarding and telnet
ip start gated
ip start telnetd
```

Warning — Do not destroy your existing startup file.

2. Reset the router to apply the filters.

When you install *NetStalker* using default values, the entire collection of common filters is installed on the router. Figure 2-2 shows which filters are nested into collections of filters and describes the use of the filters.

TABLE 2-2 Collection of *NetStalker* PCF Filters

Collection or Filter name			Description	Default Status
netstalker			Collection of the common filters	
	stalker_shun		ip addresses blocked by *NetStalker*	Dynamic
	stalker_sig		Collection of filters required by *NetStalker* signatures	
		stalker_satan_tcp	Some of the ports used by SATAN's normal and heavy scans	Applied
		sstalker_satan_udp	Some of the ports used by SATAN's normal and heavy scans	Applied
	stalker_deny_fail		Collection of filters to deny services	
		port_deny_fail	Common ports to block access to the router (ftp, r commands, and X)	Not applied
		stalker_fragmented_ header_fail	Denies packets with fragmented headers	Applied
		source_route_fail	Source routing packets should always be blocked	Applied
	stalker_watch		Collection of filters to watch interesting traffic	
		stalker_smtp_watch	Watches full traffic of the mail port	Not applied
		stalker_ftp_watch	Watches traffic of the ftp control port	Applied
		stalker_r_cmd_watch	Watches full traffic of the r commands	Applied
		stalker_audit_session	Watches for all connection requests	Applied
		stalker_x_watch	Watches full traffic of X sessions	Not applied
		stalker_ftp_data_watch	Watches full traffic of ftp data ports	Not applied
		stalker_nfs_watch	Watches nfs and portmapper traffic	Applied
stalker_ip_ spoof			Looks for source addresses that match an inside address	Applied

The previous instructions allow you to set up one router on the *NetStalker* server. To add other routers to the server, re-run the installation script for each additional router.

Starting and Stopping *NetStalker*

Starting Netstalker To start *NetStalker* do the following:

1. Login as an authorized *NetStalker* user.
   Type **%login netstalker** and press **Enter**.

2. At the UNIX system prompt type `cd $NETSTALKERHOME/bin` and press **Enter**.
3. Type `./netstlkr` and press **Enter**. The About *NetStalker* window is displayed.

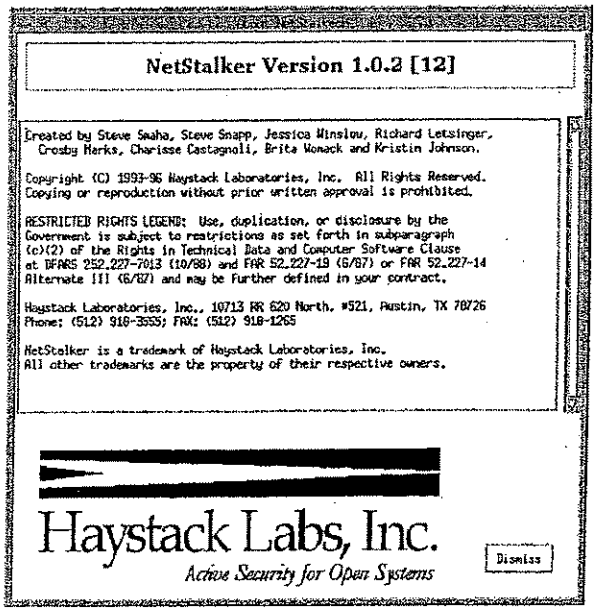

FIGURE 2-1 About *NetStalker* window

4. After reading the licensing information in the About *NetStalker* window, select **Dismiss** to close the window and display the *NetStalker* window.

   NetStalker is now running in command mode. It is not yet monitoring the network.

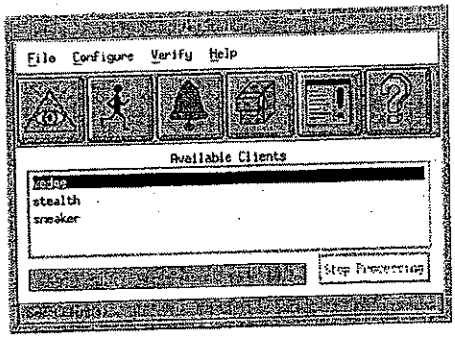

FIGURE 2-2 *NetStalker* window

- To iconify or minimize the *NetStalker* window, click on the iconify command button (the left button of the two buttons grouped on the far right side of the title bar).
- To restore the *NetStalker* window to its previous size, double click on the *NetStalker* icon.

Stopping NetStalker Generally speaking, *NetStalker* should always be running to monitor and protect the network. On the occasion when you want to stop the program,

1. From the *NetStalker* Menu bar, select **File**.
2. Select **Exit** to quit the program.

Learning About *NetStalker* Menus

This section describes the windows and menus you will see as you use the program. You can read through this section now or you can move on to the typical tasks you will perform as you use the program referring to this section as needed.

TABLE 2-3 *NetStalker* Window Menu Items

Menu Bar Item	Tool Bar Icon	Drop down Menu Item	Description
File			
		Process data	Run the current *NetStalker* configuration and report results.
		Exit	Close and exit *NetStalker*.
Configure			
		Client Information	
		Misuse Detector	Create or modify Misuse Detector configurations.
		Alarm Handlers	Create or modify alarm configurations.
		Log Manager	Create and manage event data.
		Network Addresses	Create and manage lists of network addresses.
		Show/Hide Status Window	Display or hide the *NetStalker* status window: error messages, warnings, and system status.
Verify			
		Client Access	Verify availability of the router to *NetStalker*.
		Client Info	Verify router type, name, and other data.
		Client Directory	Verify the location of the router disk.
		Client Filters	Verify which PCF filters are installed on a router.
Help			
		About *NetStalker*	Display version and copyright information.
		Windows Help	Provide information about how to use *NetStalker*'s windowing system.
		Main Menu Help	Introduce the functions available through the main menu.
		Help Topics	Display a list of all help topics. Select the desired topic to display the help text.

CHAPTER 3

Adding Router Information to *NetStalker*

Before *NetStalker* can protect your network, you must configure the program for your site by setting up the routers to be monitored. This chapter describes how to add and edit client routers listed in the *NetStalker* window. It also describes how to verify the client information.

Configuring Routers

NetStalker needs to know about the routers it will manage. You must add the routers to the list that appears in the *NetStalker* window. From time to time you will update information about the routers. This section describes what you have to know before you can add a router for *NetStalker* to manage as well as the steps required to incorporate this information into the configuration.

Before You Configure

Before you configure *NetStalker* you need the following information:

- The names of the client routers
- The IP address for each of the named client routers
- The telnet password, if any, for the named routers

See Chapter 2 for details about how to get this information.

To add a router

You add to the client list all the routers that this copy of *NetStalker* can monitor.

To add a router, do the following:

1. Deselect any client router names highlighted in the *NetStalker* window.
2. From the menu bar, select **Configure**; then select **Client Information** to display the Create New Client window. Use this window to enter all the client router information.

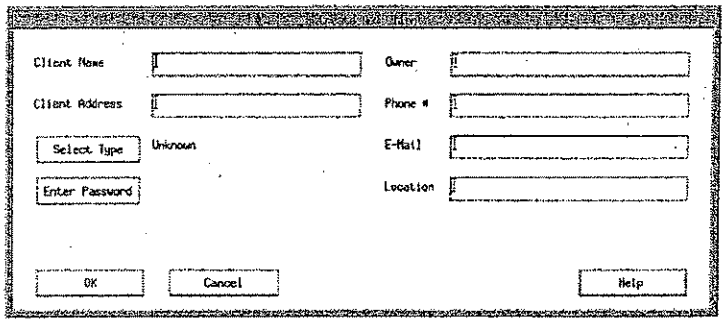

FIGURE 3-1 Create Router window

3. Consider each of the fields and button selections in the Create New Client window using the following list as your guide.

- **Client Name**: required

  To get the router name, you can open a telnet connection to the router and look for its name in the system prompt. You must use the name the router uses for itself.
- **Client Address**: required

  Use the IP address for the router.
- **Owner**: optional

  The name of the contact for the router.
- **Phone#**: optional

  The phone number of the router's owner.
- **Email**: optional

  The email address of the router owner.
- **Location**: optional

  The physical location of the router.

- **Select Client Type**: required

  Select the type of router from the Select Client Type window.

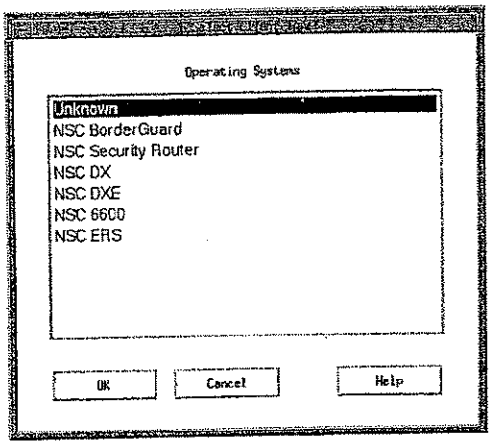

FIGURE 3-2 Select Client Type window

- **Enter Password**:

  Enter the router password in the Enter Router Password window.

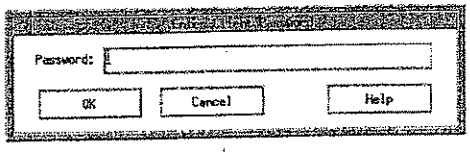

FIGURE 3-3 Enter Client Password window

Note. If you do not want to use a password for this router, clear the password field of any characters or if the field is blank, leave it blank.

4. Select **OK** to verify the password and commit your entries.

Any errors or conflicts in the new information result in an error message. The Create New Router window does not close until all errors are corrected or until you select Cancel from the window.

Note—

Note. By default, *NetStalker* stores log events in the `..data` directory on the *NetStalker* server unless another directory is specified in the Log Manager (See Chapter 7.)

Editing Router Information

As your network changes over time, you may need to edit the current router listing to reflect changes such as new router types, changed IP address, or new router password.

Editing Router Information

To edit information on an existing *NetStalker* client, do the following:

1. Select the client router in the *NetStalker* window.
2. From the menu bar select **Configure**; then select **Client Information**. The Configure Client Information window appears.

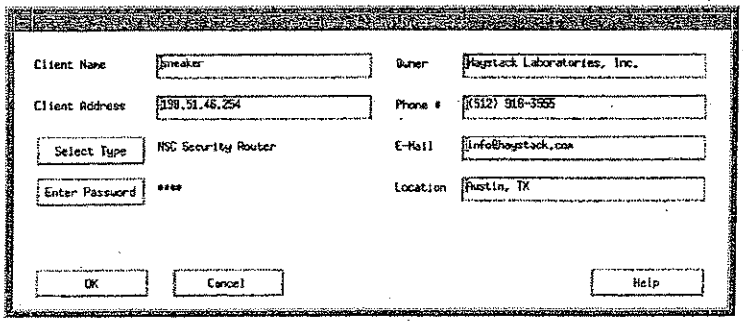

FIGURE 3-4 Configure Client Information window

3. In the Configure Client Information window, make the necessary revisions to the displayed information.
4. Select OK to save the changes.

Verifying Router Information

The next step is to verify that the client router information is accurate. This step is not required for running *NetStalker*, however we recommend that you do verify the information to ensure that all data is available to *NetStalker*.

To verify client router information, do the following:

1. In the *NetStalker* window, select the client router to be verified.
2. To display the verification options, from the menu bar select **Verify**.

Verifying Client Access

To verify the availability of the client router to *NetStalker*, select **Client Access**. *NetStalker* opens a shell that displays one of two messages, either "alive" for a completed connection or "cannot complete connection" for an unsuccessful connection.

Verifying Client Info

To verify the information about the client router, select **Client Info**. *NetStalker* opens a shell that displays the information stored about the router, such as name and type.

Verifying Client Directory

To verify that all the filters have been downloaded to the router, select **Client Directory**. *NetStalker* opens a shell that displays the contents of the startup directory on the router.

Verifying Client Filter

To verify the PCF filters that are currently active on the router, select **Client Filters**. *NetStalker* opens a shell that displays a list of the PCF filters that are applied on the router, as described in Chapter 2.

CHAPTER 4

Configuring Alarm Handlers

This chapter describes *NetStalker* alarms and how to configure them.

What are Alarms?

An alarm notifies you, the user, of an incident detected by *NetStalker*, based on reports from the router, that meets criteria you set. You may want to receive this alarm for the purpose of determining the cause or source of the event because the incident poses some "danger" to your network. In addition, you may want *NetStalker* to take an automatic action (a "response").

For each alarm generated by *NetStalker*, you can configure one or more alarm handlers to serve as communications channels from *NetStalker* to you, to other network management tools or to respond to the alarm.

Alarms come preconfigured with *NetStalker*. Generally speaking you should not change these configurations except in the following situations.

Change the configured alarms if you want to:

- Change the destination for email messages.
- Change the default destination for reports.
- Change the title of the Alarm window for screen display.
- Add your own alarms.

Configuring Alarms

You configure alarms using the Configure Alarm Handler window. This section describes each alarm type and how to configure each alarm.

To open the configuration window, from the menu bar, select **Configure** then select **Alarm Handlers**.

-Or-

Click on the  icon.

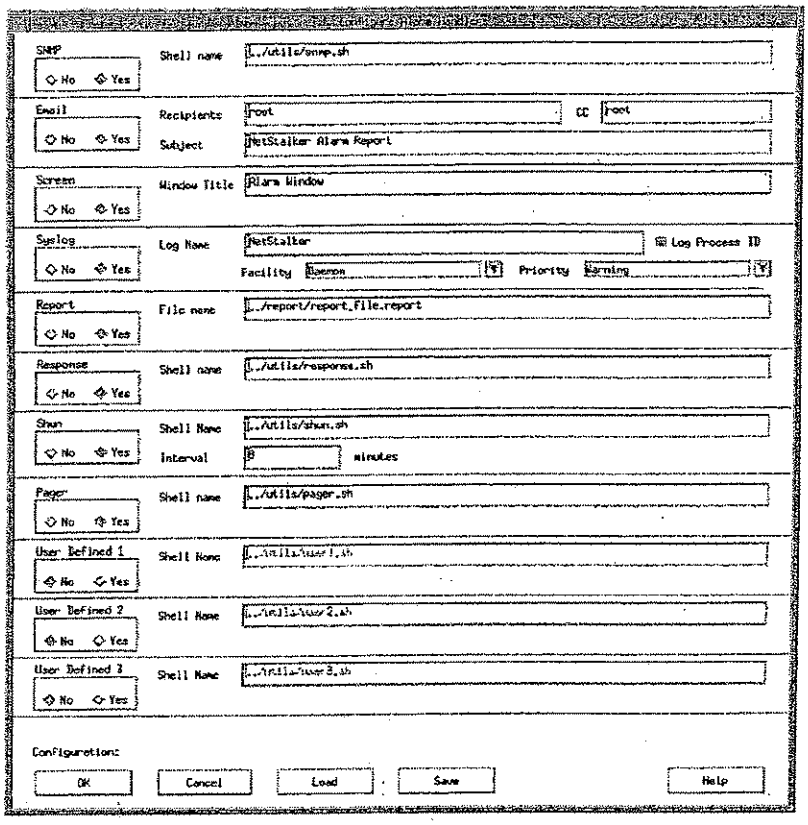

FIGURE 4-1 Configure Alarm Handlers window

There are seven default alarms supplied with *NetStalker* and you can configure three additional user-defined alarms.

Use Table 4-1 to help you select the alarms that will be active when you run *NetStalker* processes.

TABLE 4-1 A description of supplied alarms

Alarm Handler	Action when selected yes	Specify...	Default values
SNMP	Generates a site dependent SNMP (Simple Network Management Protocol) trap.	Shell name	./snmp_shell.sh
Email	Sends Email to specified parties	Recipient Email addresses Courtesy copies to additional recipients Subject line of Email message	root root NetStalker alarm report
Screen	Alarms appear in a window at the *NetStalker* console	Window name	Alarm Window
Syslog	Writes the alarm information to the system defined log location.	Name of system log Enable processid to record NetStalker ID in syslog) Facilities Severities	Log name: NetStalker Processid: [enabled] Facility: daemon Severity: warning
Report	Writes the alarm information to a file. For each new report an extension is added to the initial filename. The extension is incremented for each new report. For example report_file.1, report_file.2.	Path and file name of the first report.	./report/report_file.report
Response	Provides a general purpose response to activities taking place on the network [reserved for future use]	Shell name for the response	./response_shell.sh

Alarm Handler	Action when selected yes	Specify...	Default values
Shun	Using the address of the source that triggered the alarm, blocks the source from going through the protected router for a specified period of time.	Shell name for the executable file that initiates the protection. Period of time that the source is blocked from going through the router	Shell name: ./shun_shell.sh Time: 8 minutes
Pager	Initiates a call to specified pager numbers	Shell name of the executable file that initiates pager calls	Site dependent

Saving Alarm Configurations

After modifying an alarm configuration, you permanently save it using the **Save** button.

When you select **OK** after changing an alarm configuration, *NetStalker* prompts you to determine if you want the change to become the default configuration.

Answer **yes** to save the change and make it the default for future sessions.

Answer **no** to discard the change.

User Defined Alarms

You can create up to three user-defined shells to activate unique alarm or response mechanisms for your site. The alarms can be as simple as sending a beep to the system console or more complex such as logging the event in syslog.

To create a user-defined alarm, do the following:

1. At the operating system level, create a shell with the commands to implement the alarm. For example, you may wish to store an event in a database.
2. In the *NetStalker* Configure Alarm Handlers window, select **Yes** in the User-Defined box.
3. Type the shell name and the complete path to the shell name.

When you turn on the user-defined alarm as explained in Chapter 5, *NetStalker* automatically calls the shell and supplies the complete data for the router event.

The format for a call to any shell is the shell name, followed by a list of arguments. The arguments are listed from "a" through "p" and "A" through "B," as defined in Figure 4-2 below.

An example call from *NetStalker* is:

```
shell -a "John Doe" -b "555-1234" -c "myrouter"...
```

TABLE 4-2 Arguments for User-defined Alarm Shells

flag	data following flag
"a"	contact
"b"	phone
"c"	router name
"d"	router addr
"e"	alarm type
"f"	alarm severity
"g"	alarm message
"h"	time
"i"	event type
"j"	icmp type
"k"	source address
"l"	source port
"m"	destination address
"n"	destination port
"o"	filter name
"p"	router password
"A"	optional argument 1
"B"	optional argument 2

CHAPTER 5

Running *NetStalker*

This chapter describes the steps required to use the pre-defined configurations that are shipped with *NetStalker* and to start the *NetStalker* processes.

Scenario number	Configuration Name	Purpose	Default Output
5	r_command_watch	Monitor and record all r-comm command connections including rsh, rlogin, and rexec	To report file
4	IP_Spoof	Look for any outside machines masquerading as a machine on the inside	To report file
	Audit_TCP_sessions	Keep track of actual and attempted connections	To report file
	Blocked_fragmented_TCP_headers	Reports all blocked fragmented TCP headers	To screen and report file
	Suspicious_IP_options	Reports all ICMP source route redirect requests	To screen and report file

To Modify an Alarm Type

After deciding which *NetStalker* configurations you need to run, you may change the type of alarm generated and other alarm parameters for each configuration. To make these changes, do the following:

1. In the *NetStalker* window, deselect any routers that are selected.
2. From the menu bar select **Configure** then select **Misuse Detector.**
   -Or-
   Click on the  icon.

   The Configure Misuse Detector window is displayed.

Alarm Type	Description
Syslog	Sends the message to a system-defined log location, such as to the console or another log.
Screen	Sends the message statement to a popup Alarm Window
Report	Writes event information to a consolidated report file in a default format with each event listed by severity. Note. All configurations share the same report file.
Response	Reserved for future use.
Shun	Blocks the source IP address from using the router. Be careful what is shunned. You may block yourself.
Pager	Call a script to dial your pager number. The script is site dependent.
User Defined 1, 2, 3	User defined responses for different incidents.

6. To override the default parameters, select **Configure** in the Alarm Handlers section of the window and then modify the defaults. The alarm parameters are described in Table 5-3.

TABLE 5-3 Description of alarm parameters.

Alarm Parameter	Description
Message	General description of the captured event or message for display in the report.
Severity	User-defined severity of the event ranging from 1 = low to 10 = high.
Threshold	Count - Number of events recognized before triggering an alarm. Reset to 0 after alarm is triggered. Reset Interval - Number of elapsed seconds before resetting the counter.
Event Trace	Yes or No - Display a list of all events that triggered the alarm.
Threshold events by	All - Count all generated events to determine if threshold is met. Address - Count generated events by network address to determine if threshold is met.

7. Select **Save** to store the changes to the configuration.

   You may use the same configuration name or create a new name.
8. Check **Save as Template** to make the new configuration available for all routers.

2. From the menu bar, select **File** then select **Process Data**.
   -Or-
   Click on the  icon.

   The Run *NetStalker* window showing the list of available configurations is displayed.

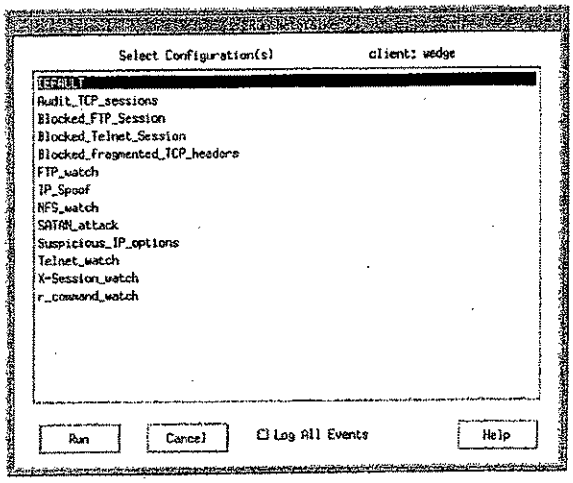

FIGURE 5-2 Run *NetStalker* window

3. Select one or more configuration names that correspond to the desired scenario or monitoring configuration.
4. If you wish to keep the event data for future review, check **Log All Events** to store the data in a file. You should next use Log Manager to establish storage locations for the data, as described in Chapter 7.
5. To begin monitoring, select **Run**.

   NetStalker immediately begins processing the events from the selected routers. The message line in the *NetStalker* window displays the monitoring status, showing the time and date of the last event processed and the total number of events processed (Figure 5-3).

CHAPTER 6

Configuring Misuse Detector

This chapter discusses how to configure Misuse Detector to detect and respond to attacks on your network.

Why Use Misuse Detector?

You use Configure Misuse Detector to create custom detection configurations to meet your needs for monitoring and responding to network activities.

You also use Configure Misuse Detector to apply alarm types to the predefined configurations, as described in Chapter 5.

How Misuse Detector Works

Misuse Detector combines a series of filters to "sieve" the router event data with a very efficient pattern matching signature analysis engine. Each filter reduces the total number of events sent to the next filter. The result is a set of all events that match the specified filters. An alarm is generated if specified thresholds are met.

For example, you could obtain a report of all network events coming from the source hacker.com that involves ftp events. You can use this report to pinpoint any suspicious activities requiring further investigation. Figure 6-1 shows the conceptual design of Misuse Detector.

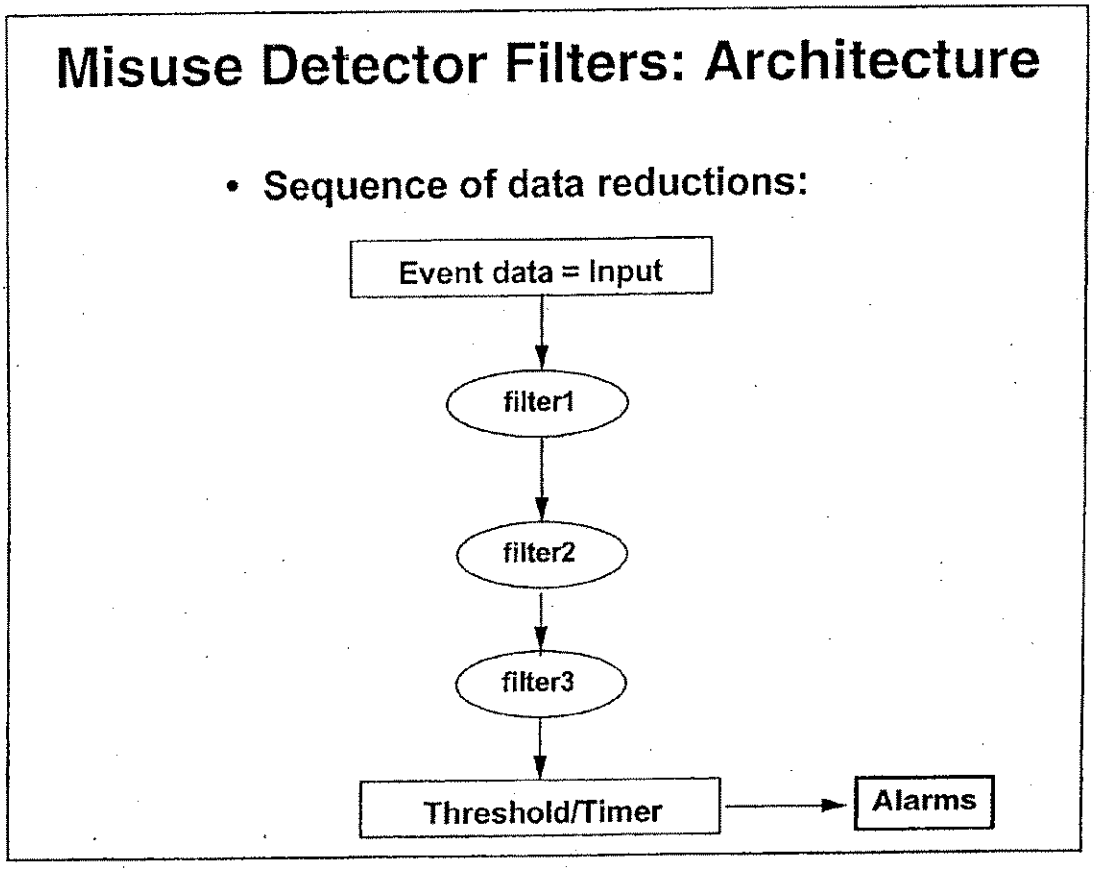

FIGURE 6-1 Misuse Detector Conceptual Design

It is not necessary to configure all filters. Filters may be set to

- Include events with specific characteristics
- Exclude events with specific characteristics
- Turn off the filter.

There are three general steps that you must take to use Misuse Detector.

1. Select the router.
2. Configure Misuse Detector filters and signatures.
3. Select the alarm type and assign parameters for triggering the alarm.

Before you start to configure Misuse Detector, here is an explanation of command buttons you will find in windows associated with Misuse Detector.

Buttons in the Windows Associated with Misuse Detector

Save

You can store frequently used configurations for Misuse Detector for future use. Selecting **Save** displays a window for naming and storing the configuration. You can use a previously defined name or type a new name.

If groups are available, you assign the new configuration to a group. If you select **Cancel**, the new configuration will automatically be assigned to the "others" group, which is a reserved group name.

Save as template

You can also save configurations as general examples for use on multiple routers by selecting **Save as template**. These configurations are shown with a template indicator when retrieved.

Load

Use **Load** to display a list of available configurations and associated groups. Selecting a group displays all configurations assigned to the group.

NetStalker comes with predefined default configurations. The DEFAULT template group and/or a DEFAULT configuration in the selected group are the first items displayed in the list and are automatically selected. All configurations not associated with a group are listed under the template group "others," which is a reserved group name.

Select All, Select None

NetStalker uses **Select All** and **Select None** to manage selections from large lists. Selecting **Select All** chooses all items displayed in the current list. **Select None** deselects any previously selected items allowing you to then select individual items.

Remove

Deletes currently selected items.

Configure Misuse Detector Window

Before you start configuring, consider the Configure Misuse Detector window illustrated in Figure 6-2.

To open the Configure Misuse Detector window,

1. Select a client router from the list displayed in the *NetStalker* window.
2. From the menu bar, select **Configure** then select **Misuse Detector** to open the window.
   -Or-
   Click on the  icon.

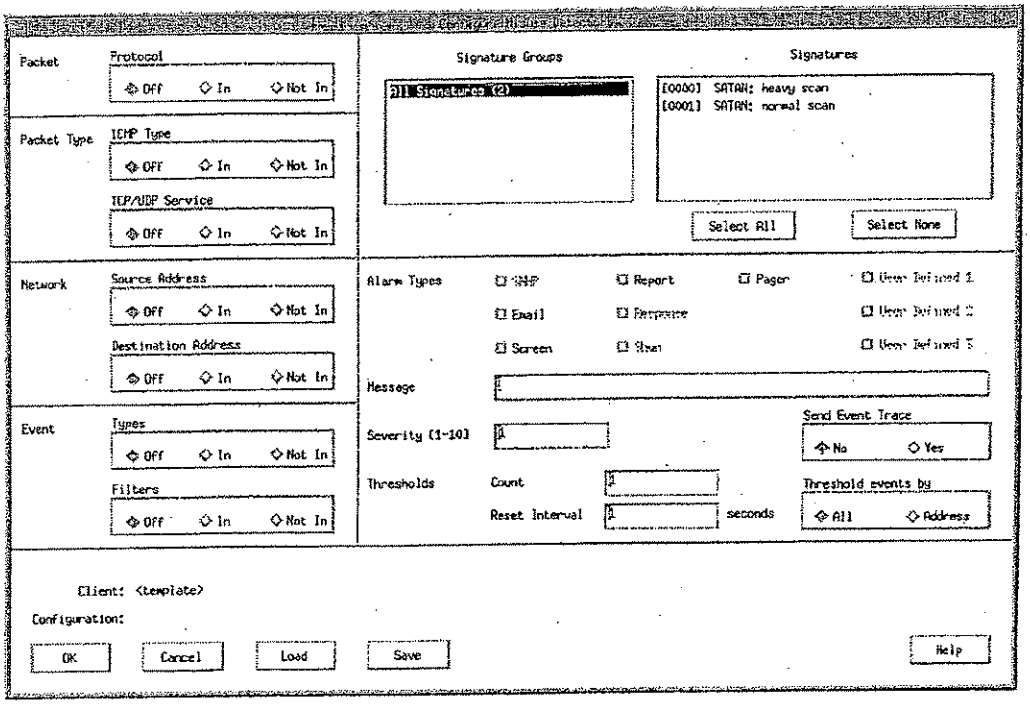

FIGURE 6-2 Configure Misuse Detector window

There are four filters included in the Misuse Detector window. The filters are

- Packet
- Packet Type
- Network
- Event

The window also contains lists of Misuse Signature Groups, Misuse Detection Signatures, and Alarm Types.

Configuring Misuse Detector

To configure Misuse Detector for the selected client router, do the following:

1. Set the desired condition for each filter in the Misuse Detector window.
   - Or -
   Load a saved configuration
2. Save a configuration that you want to use again.
   -Or-
   Save the change to an existing configuration.

Understanding the Filters

The data gathering filters (packet, packet type, network, and events) have three conditions: Off, In, and Not In. Table 6-1 describes these conditions.

TABLE 6-1 Filter conditions -- only one can be chosen.

Filter Conditions	Explanation
Off	The filter is not selected for use.
In	The filter is selected for use and filters for conditions inside your network.
Not In	The filter is selected for use and filters for conditions not inside your network.

Packet

Protocol

The Packet filter queries the events by the protocol used to transmit the packet. When you select the Protocol filter, the Select Internet Protocols window is displayed (Figure 6-3). Select from the list of available network protocols, which includes ip, icmp, ggp, tcp, egp, pup, udp, hmp, xns-idp, and rdp. For example, when you select tcp from the list, all events using the tcp protocols including telnet and ftp are returned, but no events using any other protocol are returned.

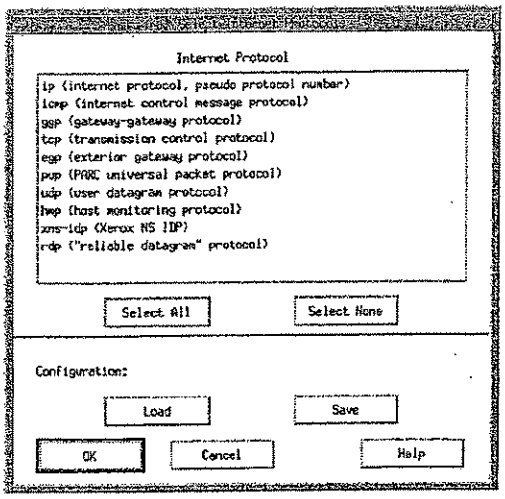

FIGURE 6-3 Select Internet Protocols window

Packet Type

The Packet Type filter queries the events by ICMP type, TCP service, or UDP service.

ICMP Type

When you select ICMP Type, the Select ICMP Packets by Type window is displayed (Figure 6-4). Select from the Object Type list, which includes echo reply, destination unreachable, source quench, redirect, echo request, time exceeded for a datagram, parameter problem on a datagram, time stamp request, time stamp reply, and information request.

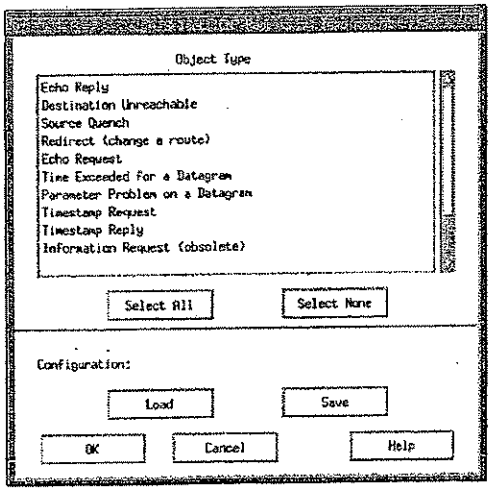

FIGURE 6-4 Select ICMP Packets by Type window

TCP/UDP Service When you select TCP Service or UDP Service, the List Network Ports window is displayed (Figure 6-5). Select from the list of Internet services such as systat, ftp, telnet, www, and Gopher. By selecting appropriate services, you can closely watch specific network activity.

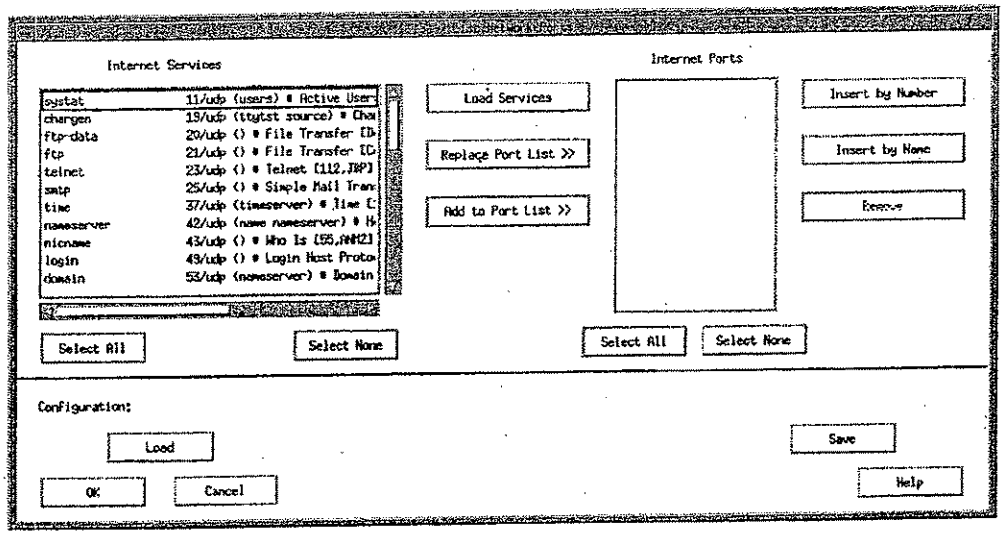

FIGURE 6-5 List Network Ports window

Once you have selected from the Internet Services display list, you may replace or add these services to the Internet Ports display list. *NetStalker* filters for the services listed in the Internet Ports list.

You may add ports to the Internet Ports list at any time. To add ports to the list

1. Select **Insert by Number**
   -Or-
   Select **Insert by Name**

2. Complete the information shown in Figure 6-6 "Specify Port(s) by Name window' or Figure 6-7 "Specify Port(s) by Number window."

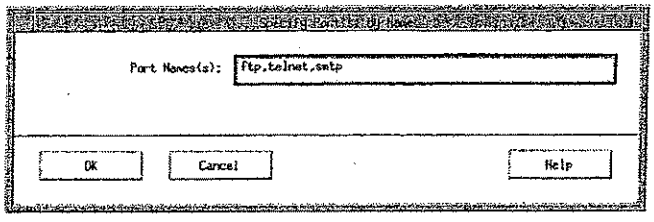

FIGURE 6-6 Specify Port(s) by Name window

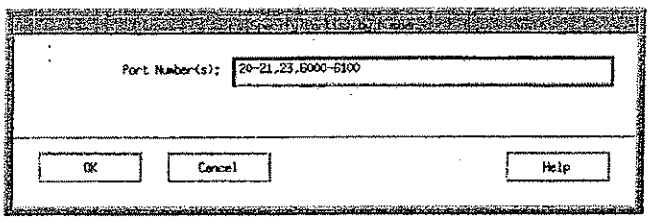

FIGURE 6-7 Specify Port(s) by Number window

To display additional services to monitor, you can load a longer list by selecting **Load Services** to display the Load Configuration window (Figure 6-8). Then select Kitchen Sink.

To create several lists of Internal Ports, select **Save** to save the lists as named objects in the database.

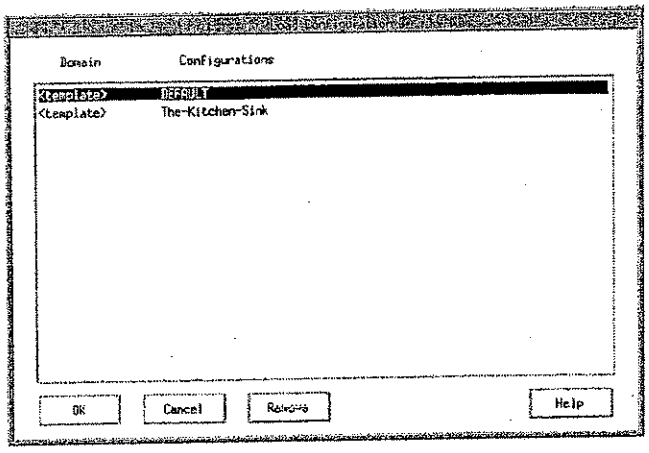

FIGURE 6-8 Load Configuration window

Network

The Network filter queries events based on the origin or destination of the connection to the router using the network address for internal or external connections. Network addresses contain the individual addresses, the classes of the addresses, and sets of individuals/classes.

Source Address The Source Address filter examines router events for the origination of the event. For example, by using Not In for Network Source Address you can filter out events generated by your internal network connections and look at events generated by external connections only.

Destination Address The Destination Address filter examines router events for the recipient of the router event. For example, you can filter out all the events that are sent directly to the router by selecting **Destination Address Not In** and the router address.

To select a Network filter, do the following:

1. From the Network section of the Configure Misuse Detector window, select **Source Address** (In or Not In) or **Destination Address** (In or Not In) to open the List Network Addresses window.
2. Accept or modify the displayed list.
   -Or-
   Select **Load** to view a stored network address list.

To modify the displayed list of addresses, select **Insert by Address**, **Insert by Hostname**, or **Remove**. The network address must be in the standard Internet address format a.b.c.d. or it can contain wildcard characters ("*"). When you insert an address by router name, *NetStalker* looks up the associated address using locally-configured network services, and displays both name and address in the list. Similarly when you insert a network address, *NetStalker* loads up the associated router name and displays both the name and address in the list.

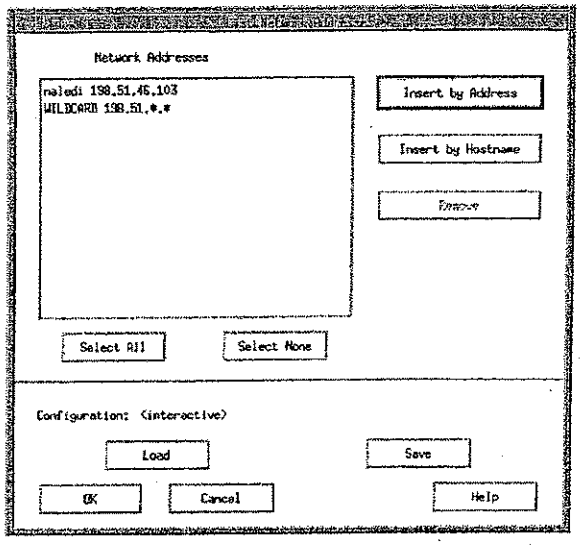

FIGURE 6-9 List Network Addresses window

Creating Network Address Lists

Network address lists are custom lists of network addresses for all accessible computers. Using named Network Addresses lists speeds up processing by limiting the amount of available data. Here are some examples of useful address lists:

- All routers being managed by this *NetStalker* server
- The *NetStalker* host
- Internal subnets or physical networks
- External corporate subnets, such as remote offices

To create lists of Network Addresses, do the following:

1. In the *NetStalker* window, select a client router.

2. From the menu bar, select **Configure** then select **Network Addresses** to display the List Network Addresses window (Figure 6-10).
3. Load the list you wish to modify.
   -Or-
   Create a new list and save it.

You can modify the existing Network Addresses list by using **Insert by Address** or **Insert by Name** or **Remove**. *NetStalker* looks up the client name or address associated with the entry and asks you to verify the selection. The new entry appears at the bottom of the Network Addresses list.

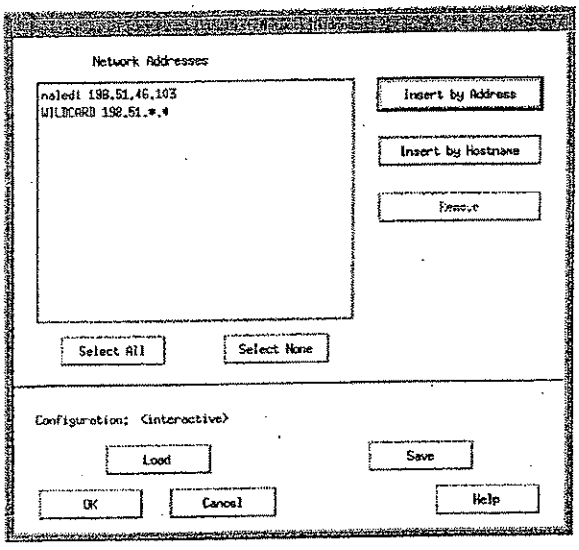

FIGURE 6-10 List Network Addresses window

Events

The Events filters query the router events based on router event types or PCF filters installed at the router.

Types

The Event Types filter examines the data for specific events or classes of events. When you select Event Types, the Configure Event Types window is displayed (Figure 6-11). Ten event classes are listed, of which nine are for router events and one is for PCF filter events. For more information about router event types, see the NSC manual for your router.

You can select each event class individually or each event type individually. If you select an event class, the associated event types are automatically selected.

Use the Select check box to confirm your selection of classes or types.

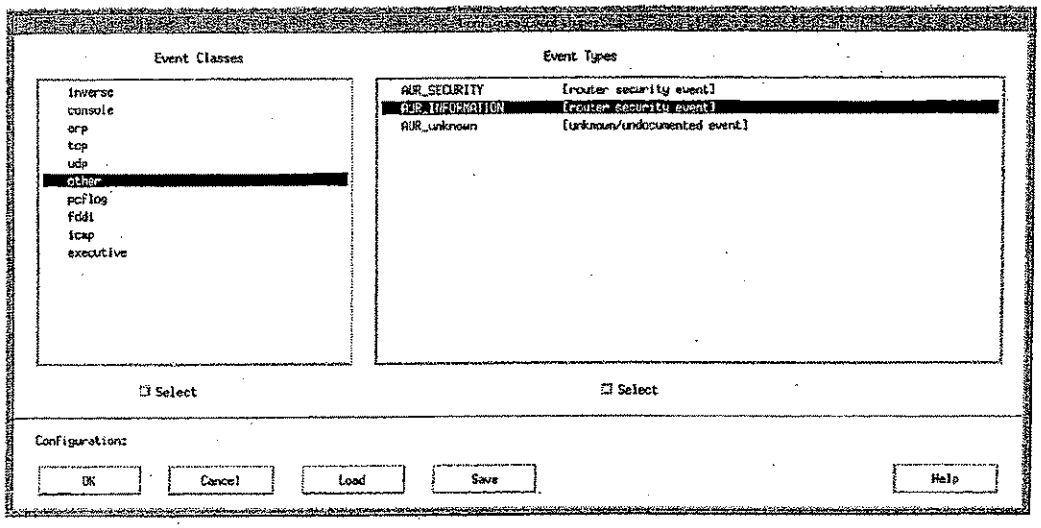

FIGURE 6-11 Configure Event Types window

Filters

Use Filters to examine all events associated with the PCF filters. When you select **Filters**, the List Objects by Name window is displayed (Figure 6-12) with a list of all PCF filters. (See Chapter 2 for a description of these filters.) You can create a list of filters by using **Insert** or **Remove**. *NetStalker* searches for these names in the event stream and returns the event when a match occurs.

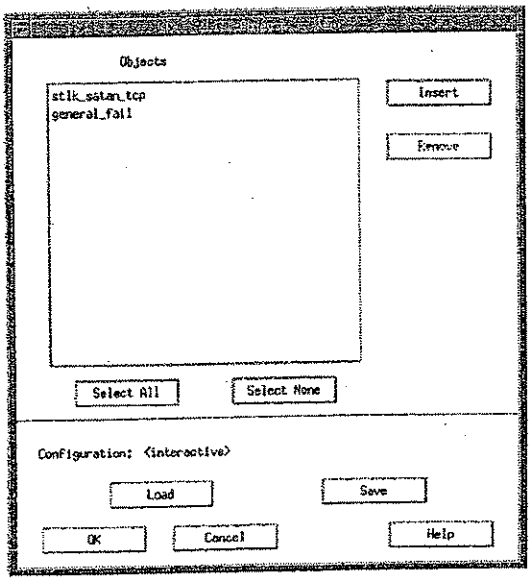

FIGURE 6-12 List Objects by Name window

Understanding Misuse Detector Signatures

Misuse Detector analyzes events for evidence of misuse or misuse "signatures." Misuse is defined as any activity that would be deemed unacceptable and undesirable were it known to the party responsible for the security of the machine. It uses Haystack Labs' proprietary database of misuse signatures of:

- Known attacks
- Attempts to exploit known system vulnerabilities
- Typical outcomes of system attacks.

Including known outcomes of attacks provides a "safety net" to capture misuse that results from attacks not represented in the set of known signatures. The misuse signatures are obtained from a variety of sources including organizations that have been targets of misuse. The results are an identified misuse and a set of events that constitute the identified misuse.

Misuse Signature Groups

The Misuse Signature Groups list in the Configure Misuse Detector window displays a list of the defined categories of misuse signatures. Selecting a group displays all signatures in the group.

Misuse Detection Signatures

The Misuse Detection Signatures list in the Configure Misuse Detector window displays a list of the currently supported misuse signatures for the selected group. You can select one or more signatures for analysis. Use **Select All** to choose all displayed signatures. **Select None** clears all displayed selections and lets you select individual signatures.

Alarm Types

The next step in creating a custom misuse detection configuration is to select one or more alarms and to assign the parameters for triggering the alarm.

In the Configure Alarm Handler window, you created the alarm configurations (See Chapter 4). In the Configure Misuse Detector window, you activate the alarms for specified Misuse Detector configurations.

To activate an alarm, select the alarm type from the displayed list.

SNMP Simple Network Management Protocol—calls a shell to send an SNMP trap. The results of that trap is dependent on your site.

Email Sends an email message containing the message, severity, and trace (if requested) to the user via Unix mail.

Screen Sends the message statement to a popup Alarm Window, shown in Figure 6-13.

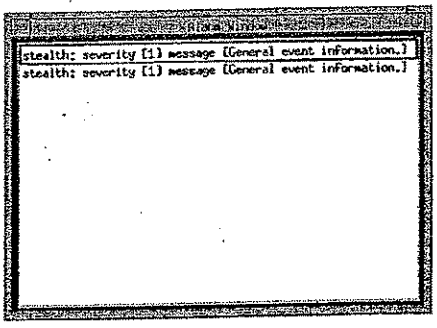

FIGURE 6-13 Alarm Window

Report Writes event information to a single report file in a default format with each event listed by severity. The default format is illustrated in Figure 6-14.

```
Router: [stealth] severity: [1]
message: [send cops]
event list: [1] events
Time = 11/15/95 11:40:06 [0], Event = NSC_PCFLOG(33000),
Source = 144.51.17.1(1083)(Hostname = calvin), Destination = 198.51.46.103(21)
(Hostname = naledi), IPprotocolType = tcp(6), Filter = report2,
Packet = E.(..T..:....3...3.g.;..\O.....P....s..
-------------------------------------------------------------------------
Router: [stealth] severity: [1]
message: [General event information.]
event list: [1] events
Time = 11/15/95 11:52:30 [0], Event = NSC_PCFLOG(33000),
Source = 144.51.17.1(1095)(Hostname = calvin), Destination = 198.51.46.103(21)
(Hostname = naledi), IPprotocolType = tcp(6), Filter = report2,
Packet = E..(....:....3...3.g.G..a.d;v...P.......
-------------------------------------------------------------------------
```

FIGURE 6-14 Default report file format

Response Reserved for future use.

Shun Blocks the source IP address from using the router. Be careful what is shunned. You may block yourself.

Pager Call a script to dial your pager number. The script is completely site dependent.

User Defined 1, 2, 3 User defined responses for different incidents.

Next, assign parameters to the selected alarms or modify the displayed defaults. If more than one alarm type is selected, the parameters apply to all alarm types.

Message Type a general description of the captured event or a message for display in the report.

Severity User defined severity level of the event ranging from 1=low to 10=high.

Threshold	**Count**–number of events to be recognized before triggering an alarm. **Reset Interval**—Number of seconds before resetting the counter.
Event Trace	**Yes** or **No**–Display a list of all events that triggered this alarm.
Threshold events by	**All**–Count all generated events to determine if threshold is reached. **Address**–Count generated events by network address and use these counts to determine if threshold is reached for a network address.

Saving Misuse Detector Configurations

Finally, save the Misuse Detector configuration for future use. To do this,

1. Select **Save** to store the changes to the configuration.

   Create a name for the new configuration.
2. Check **Save as Template** to make the new configuration available for all routers.

To Run *NetStalker*

After creating Misuse Detector configurations, you are ready to turn on the monitoring capabilities of *NetStalker*. To do so, follow these steps:

1. In the *NetStalker* window, select the router(s) to be monitored.
2. From the menu bar, select **File** then select **Process Data**.
   -Or-
   Click on the  icon.

   The Run *NetStalker* window showing the list of available configurations is displayed.

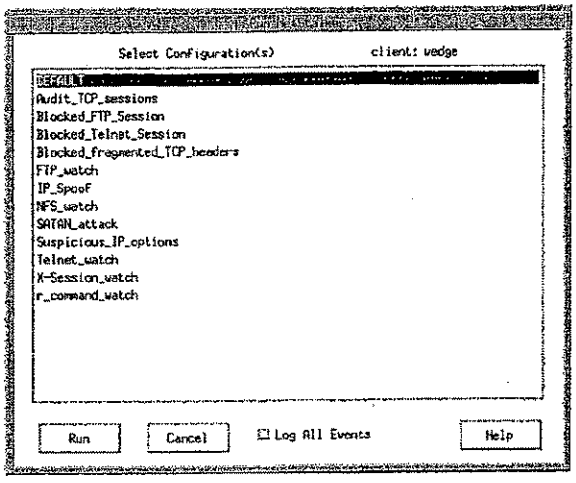

FIGURE 6-15 Run *NetStalker* window

3. Select the desired monitoring configuration name.
4. If you wish to keep the event data for future review, check **Log All Events** to store the data in a file. You should next use Log Manager to establish storage locations for the data, as described in Chapter 7.
5. To begin monitoring, select **Run**.

   NetStalker immediately processing the events from the selected routers. The message line in the main menu displays the monitoring status, showing the time and date of the last event processed and the total number of events processed.

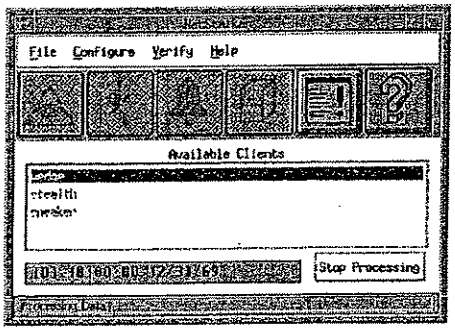

FIGURE 6-16 *NetStalker* window with status lines

6. You will receive the alarms you selected when suspicious activities are detected.

CHAPTER 7

Managing and Analyzing Log Files

This chapter describes how to manage and analyze historical router event data.

When you selected Log All Events in the Run *NetStalker* window, *NetStalker* automatically started saving the router events to a default location. The next steps are to manage the log data using Log Manager and then to analyze the data in *NetStalker*.

Log Manager controls the long-term retention of event files across the network. Log Manager implements network-wide storage policies using a hierarchy of directories, conditions for moving log files to the directories, and operations performed on the files.

Log Manager migrates log files through a user-defined hierarchy of locations using existing backup and archive policies based on:

- file age
- current disk capacity

Hierarchy

Log Manager establishes a hierarchy of locations for storing files and predetermined criteria for moving files to the locations. They are displayed in order of precedence of movement, with the first one the primary location in the hierarchy. An unlimited number of locations may be entered, although more than five locations may be unmanageable. Locations may be local drives, tape drives, or remote archived storage, so long as they are available across the network using the NFS or an equivalent protocol. Figure 7-1 represents a graphical view of hierarchical file management:

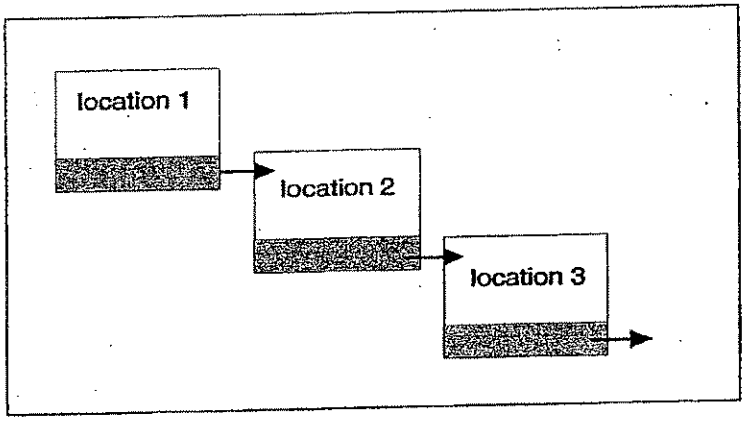

FIGURE 7-1 Log Manager's Conceptual Design

Making Changes

Most users will not need to change the Log Manager configuration after it has been initially established. *NetStalker's* template feature implements network-wide policy changes in storing event data on routers.

1. In the *NetStalker* window, select the client router to be configured.
2. From the menu bar, select **Configure,** then select **Log Manager.**
   -Or-
   Click on the  icon.

   The Log Manager window is displayed.

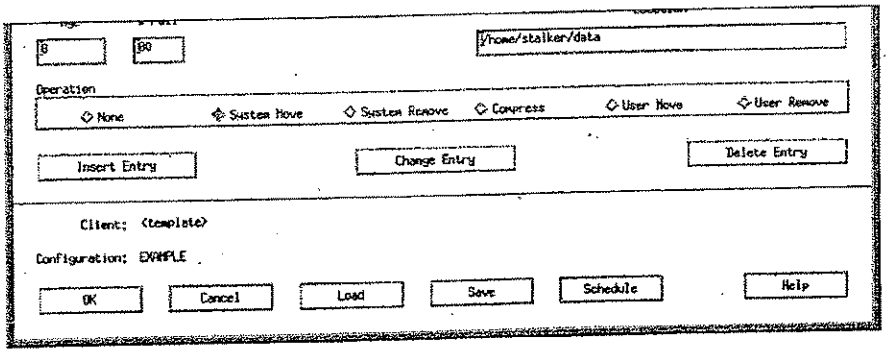

FIGURE 7-2 Configure Log Manager window

This window has several functions:

System Storage Management

When **System On** is selected, the Log Manager moves log files into the specified locations for any active routers. The default setting is **System Off** which tells the Log Manager not to move log files into the specified storage locations for any routers.

```
Enhanced Xerox PostScript Error Handler  v1.5  Mon Oct 12 8:00 am 1992

ERROR: rangecheck
OFFENDING COMMAND: put

THE OBJECTS ON THE TOP OF THE OPERAND STACK WERE:
167
792
àà°°°°ddÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿØÿÿÿØÿØÿÿÿØÿØÿÿÿØÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
--nostringval--

THE SOURCE LINES FOLLOWING THE ERROR ARE:
ffff8cebffffe0fdb0f0fcff0000feff0000f9ff0000fcff1f0000feff0ff0000feff0ff0000feff
0000feff0000feff0000feffeff0ff008f64ebffffcca7ffff8ce9ffffcca7ff0000f9ff0000fcff
1f0000feff0ff0000feff0f0ffdcffff27ffff8ce9ffffcca7ffff8ce9ffffcca7ffff8cb9ffffcc
a7ffe0fdb0ff64ebf0ff80ffffffccafeff0200ff00fb0080ffdcfffe8c00cc80ff80fffbff80ff
fffffccaf0ffdcffff1f8cb9ffffcca7ffff8cebffffe0fdb0ff64

ffe0fdb0ff64ebffa4cc03ff00ff0080f880ffbdffffccebffffe0fdb0ff64

ffe0fdb0ff64ebffc28c00cce9ffd440ff64ebffff8c0db0ff64


EXTRA INFORMATION TO AID IN DEBUGGING THIS ERROR:

PostScript:  rangecheck:

A numeric operand's value is outside the range expected by an operator.

Details:

A numeric operand's value is outside the range expected by an operator.
For example, an array or string index is out of bounds, or a negative number
appears where a non-negative number is required.  rangecheck can also occur
if a matrix operand does not contain exactly six elements.

Recovery:

Check operand's value against required parameters to the operator and
defined value of data type (ex: check defined length of an array in
question).
```

APPENDIX A

Troubleshooting Guide

Error Handling

NetStalker was designed to detect and correct most problems that may arise. In unusual circumstances when a fatal error occurs, an Application Error window appears on the screen. To ensure the integrity of your *NetStalker* installation, please complete the information in the enclosed form when you install and upgrade *NetStalker*. Please record the error information on the Software Problem Report form included in this appendix and return it to technical support.

To Recover From Errors and Malfunctions

In general, the program handles fatal errors by writing an explanatory message to its error log file prior to terminating. The error log file is **$NetStalkerHOME/bin/ CURRENT_DATE.log** where **CURRENT_DATE** may take the form 01Jun94. For example, *NetStalker* does a report/abort sequence if no disk space is available for the user.

Problem:	*NetStalker* does not seem to catch the data that is coming from the router.
Diagnosis:	*NetStalker* sorts the data based on the name the router supplies. The name entered in the router/client list must be the same as on the router itself.
Fix:	Make sure the name of the router is the same as the name in the router list. This can be done by comparing the router list to the information returned by using the Verify Client Info option in the Verify menu.

Problem:	The filters have syntax errors.
Diagnosis:	There are different types of filters for your router. These are based on the level of PCF you are running. PCF version 1 is for older routers but can run on the new ones, PCF version 2 is for the new routers. Older routers will generate syntax errors when compiling newer PCF commands.
Fix:	Rerun the INSTALL.filters script to install the proper version of the router filters.

Problem:	*NetStalker* can't open an X display.
Diagnosis:	This is a common problem with X applications. Permissions must be granted on a host by host basis to use your console.
Fix:	On your console, enter "xhost +{HOSTNAME}" where {HOSTNAME} is the name of the machine where you are running *NetStalker* (this could be the same machine you are on). In the window you are running *NetStalker* from export your DISPLAY: For csh users: setenv DISPLAY {HOSTNAME}:0.0 For sh users: DISPLAY={HOSTNAME}:0.0 For ksh users: export DISPLAY={HOSTNAME}:0.0

Problem:	*NetStalker* is unable to access databases.
Diagnosis:	You need access/write privileges to the *NetStalker* databases. The permissions need to be reset.

Fix:	Change the permissions on {NETSTALKERHOME}/dbms to 770. Change permissions on the files inside to the same. `chmod -R 770 {NETSTALKERHOME}/dbms`

Problem:	*NetStalker* returns a message that it cannot connect to the router.
Diagnosis:	*NetStalker* needs specific router information in order to talk to it. These include the router name, the IP address, and the password. If any of these are wrong there may be problems talking to the router.
Fix:	Ensure the router information matches up with the router. The router name is returned by running the Client Info option in the Verify menu. The IP address and password must be obtained from your network administrator.

Problem:	On Solaris, the INSTALL script fails, saying "Unable to get ethernet address (embedkey.cpp" ...
Diagnosis:	*NetStalker* cannot find the Ethernet device named le0. Check the available ethernet devices to see if le0 is defined.
Fix:	Use the command "ifconfig -a", and see if you have an entry for le0. Even if your machine is stand-alone, it must have an IP address for Stalker to install and operate. If an entry for le0 is not present, become root and do the following. 1. Edit /etc/hostname.le0, inserting one line containing the correct IP address. 2. Edit /etc/hosts, and make sure it has an entry with the correct IP address and the hostname separated with a tab. An example of a correct line is: `129.200.0.1 adminbox` 3. Reboot the machine after everyone except root has logged off. Here is an example of how we do it: 1. Type **$ sync** and press **Enter**. 2. Type **$ init 0** and press **Enter**. This will be followed by some shutdown messages. 3. Once you are at the monitor, type **boot -r** and press **Enter**.The "**-r** option" tells the operating system to reconfigure itself. 4. If an entry for le0 is present, does it have the correct IP address?

5. If the le0 entry is present, and the ip address is incorrect, edit /etc/hostname.le0.
6. Edit /etc/hosts.
   Make sure it has an entry with the correct IP address and the hostname separated with a tab.
7. Reboot the system.

Problem: If you observe the following error message and no other copy of *NetStalker* is running:

Error: unable to execute more than one real time NetStalker

Diagnosis: Abnormal termination of *NetStalker* program, resulting in errors in environment variables.

Fix: Do the following:

1. Type `% cd $NETSTALKERHOME/bin % rm .netlock` and press **Enter**.
2. Restart *NetStalker*.

Problem: If you observe the following error message when starting *NetStalker*:

smaha@/home/smaha/hs2/src/product/bin: ./stalker.exe

Warning: Can't load Codeset file 'C', using internal fallback

Diagnosis: The incorrect environment variables are set.

Fix: Set up the environment variables to use the IXI Motif:

```
setenv XLIBI18N_PATH /usr/server/IXImd12x/lib/X11
```

Problem: Database locking difficulties.

Diagnosis: Only one real-time *NetStalker* session and one interactive *NetStalker* session can be running concurrently.

Fix: Use the save locking method for the interactive *NetStalker* session as well as the real-time *NetStalker* session. Touch the file .intlock and test it before starting an interactive *NetStalker* session.

Problem:	Report output is interleaved when running *NetStalker* both in real-time and in interactive sessions.
Diagnosis:	Interactive and real-time mode differ in alarm handler values. The report output is interleaved.
Fix:	If you want changes to be permanent, save the values from the interactive *NetStalker* session to DEFAULT-interactive.

Please record the following information each time you install or upgrade your *NetStalker* software:

Date Installed:

NetStalker Version:

netstalker Checksum:

Date Installed:

NetStalker Version:

netstalker Checksum:

Date Installed:

NetStalker Version:

netstalker Checksum:

Date Installed:

NetStalker Version:

netstalker Checksum:

Date Installed:

Stalker Version:

netstalker Checksum:

Date:_____

NetStalker™ Software User Report

☐ - Software Problem
☐ - Software Suggestion
☐ - Other (Describe Below)

Name:	Alternate Contact:	Phone#:
Email:	Fax#:	Hardware Description:
Company:		Need fix by (date):
Address:		Product version:
City:	State:	Zip:

Brief Description of Problem :

Problem severity:

_____ 1. An error which causes an unexpected program termination or which prevents the accomplishment of a critical function of the program.

_____ 2. An error which significantly and adversely affects the ability of the program to accomplish a critical function and for which there is no workaround solution.

_____ 3. An error which significantly and adversely affects the ability of the program to accomplish a critical function and for which there is a reasonable workaround solution.

_____ 4. An error which is an operator inconvenience or annoyance and which does not affect a critical program function.

_____ 5. All other errors.

Detection method (How can we detect this problem?) Pick one:

_____interactive use

_____batch use

Haystack Labs, Inc.
Software That Can Be Trusted

10713 RR 620 North, #521
Austin, Texas 78726
(512) 918-3555 (voice)
(512) 918-1265(fax)

Date:_____

Co: _____
Contact:_____
Phone:_____

Detailed problem description:
Please use this section to describe in detail your suggestions for enhancements to the product or description of a problem. If describing a problem, also describe how to reproduce it, diagnostics used, and suggested correction(s). Attach listings and screen printouts whenever possible. Use additional pages if necessary to complete your report.

Related information:
(attach files that help detect the problem, etc.)

For Haystack Labs, Inc. use only

ID Number: Date Received:
Short description:
Laboratory information:
Assigned engineer: Project phase:
Problem type:
Recommended change:
Analysis time (hrs): Est. fix time (hrs): Est. fix date:
Resolution information:
Resolution:
Changed source location(s):
Resolved by: Actual fix time (hrs): Actual fix date:

Haystack Labs, Inc.
10713 RR 620 North, #521
Austin, Texas 78726
(512) 918-3555 (voice)
(512) 918-1965 (fax)

Glossary

Alarm
Notification of an incident detected by *NetStalker* that is an event reported by the router.

Alarm handler
A feature in *NetStalker* that manages alarm configurations.

background operation
Cron jobs created by *NetStalker's* Scheduler to routinely process Log Manager configurations.

client
A router generating network events. A router whose event data is analyzed by *NetStalker.* See also "*server.*"

crontab
A standard Unix program that allows scheduling jobs for regular background operation; for further information, see `crontab(1)`, `crontab(5)`, `cron(8)`.

events
See *"router events."*

event attributes
Information logged for an audit event; includes timestamp, event type, source and destination, IP addresses and ports, and more.

filters
In *NetStalker's* Misuse Detector, a user-controlled data reduction operation; the user may request all events that pass through the filter (when the filter is marked as "IN") or all events that do not pass through the filter (when the filter is marked as "NOT IN").

incident
An instance of an attack or misuse detected by *NetStalker.*

Internet
A worldwide collection of interconnected TCP/IP networks.

IP spoof
Setting an external IP address to an address that appears to be a legitimate internal IP address so as to trick the network into believing that an attempt to logon from the external address coming from a "legitimate" node within the network.

Log Manager
A feature in *NetStalker* manages the storage of router event data.

Misuse Detector
A feature in *NetStalker* that analyzes router events for attacks and misuse.

misuse signatures
Machine-readable patterns of events used by *NetStalker's* Misuse Detector to find instances of misuse in audit data.

Network File System (NFS)
A protocol developed by Sun used to provide remote network access to files on different kinds of machines. NFS servers also provide kernels and swap files to diskless clients so they can operate.

object name
The human-readable name of an object; usually a file name or the name of a device; for example, `/etc/passwd` or `/dev/ttya`.

regular expression
A pattern matching technique used in *NetStalker* and often used in Unix; for further information, see `grep(1v) [Sun]`, `grep (1) [AIX]`.

router events
Instances of system calls or services by system utilities that are recorded in the audit trail.

server

The host on which the *NetStalker* executables are installed and which runs *NetStalker*, typically the system manager's system. The *NetStalker* server manages and analyzes router event data from one or more *NetStalker* clients. See also "*clients.*"

signature

See "*misuse signatures.*"

switchover

The process by which the audit daemon closes the current router event file and opens a new router event file in the current audit directory.

time stamp

The date and time at which an event occurs.

Index